REMARKS

Claims 1-25 were examined.

Claims 5-16 were indicated to be directed to allowable subject matter.

Claims 22-25 were objected to. Claim 23 was amended to be consistent with claims 22 and 24-25. Withdrawal of the objection is therefore solicited.

Rejection Under 35 USC 102

Claims 1-4 and 17-25 were rejected as anticipated by BARTON 6,163,842.

The present application is a National Stage application of a PCT application. Attention is drawn to the PCT Abstract which discloses that the inventive process is for secure message transmission and comprises

i) transmitting the contents of the message and its signature by the transmitter (1), and further

ii) transmitting transmitter identification information (CRYPTIDENT) and additional information deriving from the message (IDEM). In the inventive process, the receiver (2) likewise determines information deriving from the contents of the message received and compares said information against the corresponding transmitted information (IDEM) in order to validate the message in the event that they coincide.

Beginning at the bottom of specification page 10, it is further disclosed that at stages 101-102 (Figure 2), the transmitter 1 calculates a signature, whereby the signature is then attached to the contents of the message in order to create a signed message, and the encoded signed message (M,S)c is then transmitted at a stage 105 to the receiver 2 over the communication line.

The invention further provides (at stage 104) that the transmitter 1 also calculates transmission signature information IDEM that derives from the message according to a specified law. In the illustrated example, the transmitter 1 also calculates the transmitter identification information, IDENT_SPY. The combination of these pieces of information, IDEM and IDENT_SPY or CRYPT_IDENT, is also transmitted to the receiver 2. Thus, the transmitter 1 associates with the signed message transmission checking information IDEM that derives from the signed message according to the specified law, and the transmitter 1 generates and transmits to the receiver 2 data that represent the signed message and the transmission checking information IDEM, as well as, in this example, the transmitter identification information, IDENT_SPY, which personalizes the law.

Thereafter, the receiver 2 extracts from the signed message the valid contents of the message and the signature that is received. The receiver 2 then does a signature

comparison. In addition, the receiver 2 determines, according to the specified law, reception checking information IDEM' that derives from the received message, and then compares the reception checking information IDEM' against the transmission checking information IDEM in order to validate the received message in the event that they coincide.

Claim 1 has been amended consistent with this disclosure. Previously dependent claims 19 and 22 have also been amended consistent with claim 1. No new matter is entered by way of these amendments.

The embedding of authentication information with digital data, as taught by BARTON, is not the same as that recited in the independent claims.

BARTON discloses that arbitrary digital information (an authentication stamp) is embedded within a stream of digital data that is transmitted to the user, to allow a user to determine whether the digital data have been modified from their intended form (Abstract) during the transmission process. The embedded information is extracted from the received stream of digital data to verify that the original digital data stream has not been modified as modification of the transmitted digital data stream will preclude a successful signature comparison.

BARTON uses the embedded digital information to provide a means of determining whether the data stream was

modified during transmission, where modification of the data stream is indicated by an unsuccessful signature comparison.

BARTON does not disclose generating both a signature and transmission checking information, where both a signature comparison and transmission checking information comparison are performed. Because of this, BARTON only performs the signature comparison. BARON does not, in addition to the signature comparison, perform the additional transmission checking information comparison.

BARTON does not separately generate and transmit transmission checking information in that the claim 1 recitation requires the transmitter associates with the signed message transmission checking information (IDEM) deriving from the signed message according to a specified law.

BARTON does not disclose deriving associating transmission checking information from the signed message. Rather, BARTON teaches modifying the signed message based insertion of an authentication stamp. In BARTON, there is no transmission checking information associated with the signed message; there is only the modified signed message.

Claim 1 requires "-the transmitter generates and transmits (105) to the receiver data that represent the signed message and the transmission checking information (IDEM),". In BARTON there is only transmitted the signed message, where the

signed message has been modified by the insertion (embedding) of the authentication stamp.

For details of the embedding, see column 5, beginning at line 66 which discloses authenticating a block of digital data by providing an authentication stamp that is embedded into a digital block that contains a digital object. The authentication stamp modifies the data comprising the digital block. The authentication stamp may include additional data supplied by the user (meta-data) that are carried in a secure and reliable fashion and that may be retrieved from the digital data block as needed.

Upon receipt of the transmitted signed message, BARTON teaches to extract the authentication stamp (passage spanning columns 7-8). If the signed message has not been modified during transmission, the signature comparison will be successful. However, if the message has been modified during transmission, the signature comparison will not be successful. See Figure 2, steps 30, 36, 40. See also column 8, lines 14-22.

From these passages and figures, one can see that although BARTON teaches additional security, there is no teaching of a transmitter deriving transmission checking information from the signed message, the derivation being based on a specified law. Although BARTON teaches modifying the signed message by inclusion of an authentication stamp, BARTON does not teach associating with the signed message derived transmission checking

information. Although BARTON teaches a signature verification, BARTON does not teach a further step of comparing reception checking information (IDEM') against the transmission checking information (IDEM) in order to validate the message received in the event that they coincide.

BARTON this does not anticipate the independent claims.

Also, note that BARTON does not anticipate the features of claim 3 (this claim being allowed in the EP proceedings).

BARTON does not discloses that the transmitter additionally generates and transmits transmitter identification information (CRYPT_IDENT or IDENT_SPY) that was used to personalize said law, and the receiver likewise personalizes the law according to the transmitter identification information (CRYPT_IDENT or IDENT_SPY) that is received in order to determine the reception checking information.

The remaining claims are allowable at least for depending from an allowable claim.

Allowance of all the claims is therefore solicited.

This response is believed to be fully responsive and to put the case in condition for allowance. Entry of the amendment, and an early and favorable action on the merits, are earnestly requested. Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Should there be any matters that need to be resolved in the present application; the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/Roland E. Long, Jr./

Roland E. Long, Jr., Reg. No. 41,949
209 Madison Street
Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573

REL/fb